DCID 1/21

U.S. INTELLIGENCE COMMUNITY PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES

SECTION I
POLICY

A. GENERAL:

A Sensitive Compartmented Information Facility (SCIF) is an accredited area, room, group of rooms, or installations where Sensitive Compartmented Information (SCI) may be stored, used, discussed and/or electronically processed. SCIFs shall be afforded personnel access control to preclude entry by unauthorized personnel. Non-SCI indoctrinated personnel entering a SCIF must be continuously escorted by an SCI indoctrinated employee who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent as well as detect visual, acoustical, technical and physical access by unauthorized persons. Entrance doors to SCIFs must be limited to one. If extraordinary circumstances require more than one door, appropriate justification must be approved by the Cognizant Security Authority (CSA). Physical security criteria is governed by whether the SCIF is in the United States or not, and whether it is located at, above or below ground level according to the following conditions: Closed Storage, Open Storage, Continuous Operations, Secure Working Areas, Non-Discussion Areas, and Administrative/Service Areas.

B. TWO-PERSON RULE:

As a matter of policy, SCIFs should be staffed with sufficient people to deter unauthorized copying or illegal removal of SCI. Communication centers, document control areas, and like facilities that handle or store quantities of SCI must be manned while in operation by at least two appropriately indoctrinated persons in such proximity to one another as to provide mutual support in maintaining the integrity of the facility and the material stored therein. The granting of exceptions to this policy will be made a matter of

record by the CSA and should involve consideration of the proven reliability and maturity of the persons involved; the volume, variety, and sensitivity of the holdings in the facility; and whether or not the persons involved are subject to periodic polygraph examinations as a condition of access. Exceptions for communication centers, document control areas, and the like, should be granted in only extraordinary circumstances. Classified work by a lone individual in any SCIF is to be avoided. Contractors will provide two person occupancy in all SCIFs not specifically excepted by the CSA.

C. SOUND ATTENUATION:

All SCIFs must meet the sound attenuation requirements as set forth in Chapter 13 of Architectural Graphic Standards.

D. CO-UTILIZATION:

Agencies desiring to co-utilize a SCIF should accept the accreditation of the facility as determined by the CSA. Exceptions to this policy are valid only when significant deviations from DCID 1/21 standards exist or when the co-utilizing agency requires security enhancements at the facility in connection with an especially sensitive program. All proposed security enhancements must be fully coordinated with the CSA prior to implementation.

E. INSPECTIONS:

A SCIF inspection every two years by the CSA or designated representative is required to certify continued compliance with DCID 1/21; however, an annual SCIF inspection is strongly recommended.

SECTION II
DEFINITIONS

ACCESS CONTROL SYSTEM, UNATTENDED:

An electronic, electromechanical, or mechanical system designed to identify and/or admit personnel with properly authorized access to the secure area. Identification may be based on any number of factors such as the sequencing of a combination, special key, badge, fingerprints, signature, voice, etc. These systems are for personnel access control only and are not to be used for the protection of classified materials.

ACOUSTIC SECURITY:

Those security measures designed and used to deny aural access to classified information.

ADMINISTRATIVE/SERVICE AREAS:

Those identified areas within an accredited SCIF where storage, discussion, and/or processing of SCI is not allowed.

ACCREDITATION:

Formal certification by a CSA of a specific place (to be referred to as a SCIF) which meets prescribed physical and technical security standards.

AUTHORIZED PERSONNEL:

Any person who is fully cleared and indoctrinated for SCI, has a valid need to know, and has been granted access to the SCIF.

CLOSED STORAGE:

The storage of SCI material in properly secured GSA-approved security containers within an accredited SCIF when the SCIF is not occupied.

COGNIZANT SECURITY AUTHORITY (CSA):

Government Agency responsible for the accreditation of a SCIF.

CONTINUOUS OPERATIONS:

This condition exists when a facility is manned 24-hours every day by not fewer than two appropriately indoctrinated personnel who have the continuous capability of detecting unauthorized entry into the SCIF. Positive identification and access control must be maintained at all entrance points not fully secured.

CONTINUOUS PERSONNEL ACCESS CONTROL:

An access control system where access to a facility is continuously controlled by a cleared individual, as determined by the CSA.

CONTROLLED AREA:

Any area to which entry is subject to restrictions or control for security reasons.

DOCUMENT:

Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

GUARD:

A properly trained and equipped individual whose duties include the protection of a SCIF. Guards whose duties require direct access to a SCIF or patrol within a SCIF must meet the clearance criteria in Director of Central Intelligence Directive 1/14. The CSA will determine if indoctrination is required.

INTRUSION DETECTION SYSTEM:

A security alarm system consisting of various types of components (balanced magnetic switches, capacitance, infrared, ultrasonic, etc.) to detect the unauthorized entry into a facility.

NON-DISCUSSION AREA:

A clearly defined area within a SCIF where classified discussions are not authorized. All such areas shall be clearly marked.

OPEN STORAGE:

The maintenance of SCI material within a SCIF in any configuration other than within GSA-approved security containers.

SCI FACILITY (SCIF):

An accredited area, room, group of rooms, or installations where SCI may be stored, used, discussed and/or electronically processed.

SECURE WORKING AREA:

An accredited facility which is used for handling, discussing and/or processing of SCI but where SCI shall not be stored.

SENIOR OFFICIAL OF THE INTELLIGENCE COMMUNITY (SOIC):

Those senior principals and observers on the National Foreign Intelligence Board (NFIB) who head intelligence organizations or intelligence-producing agencies within the Intelligence Community (IC).

SENSITIVE COMPARTMENTED INFORMATION (SCI):

SCI is classified information concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

SOUND GROUPS:

Voice transmission attenuation groups (ratings measured in decibels-db) may be found in Chapter 13 of Architectural Graphic Standards established to satisfy the acoustical security requirements of SCIFs.

SOUND TRANSMISSION CLASS (STC):

The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.

SURREPTITIOUS ENTRY:

The unauthorized entry into a SCIF or security container in a manner in which evidence of such entry is not readily discernible.

TACTICAL OR COMBAT OPERATIONS:

Operations which are conducted under combat or simulated combat conditions (to include ground, airborne and shipboard) and which must provide for a mobile or non-permanent SCIF environment.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) SURVEYS AND INSPECTIONS:

A thorough physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration of the facility for hostile technical collection of classified and sensitive information.

TEMPORARY SECURE WORKING AREA (TSWA):

A temporarily accredited facility which is used no more than 40 hours monthly for handling, discussing, and/or processing of SCI, but where SCI shall not be stored.

VAULT:

A room(s) used for storing, handling, discussing, and/or processing SCI and constructed to afford maximum protection against unauthorized entry.

VISUAL SECURITY:

Those security measures designed and used to deny unauthorized visual access to classified materials and activity.

VOLUMETRIC SENSORS:

An alarm sensor which detects movement or human presence within a SCIF.

SECTION III
PERIMETER CONSTRUCTION CRITERIA FOR SCI FACILITIES

A. GENERAL:

Physical security criteria is governed by whether the SCIF is in the United States or not, and whether it is located at, above or below ground level according to the following conditions: Closed Storage, Open Storage, Continuous Operations, and Secure Working Areas.

B. SCI FACILITIES LOCATED IN THE UNITED STATES AT GROUND LEVEL:

1. Closed Storage

(a) The SCIF must meet the specifications as listed in Section V, A4, or meet open storage requirements. SCIFs within fenced, guarded military compounds or equivalent may use specifications specified in Section V, A2.

(b) The SCIF must be alarmed in accordance with Section IV.

(c) SCI material must be stored in GSA-approved security containers.

2. Open Storage

Open storage of SCI material shall be avoided. When open storage is necessary, the SCIF must meet either:

(a) The construction specifications for vaults set forth in Section V, A1, and must be alarmed in accordance with Section IV; or

(b) The construction specifications for SCIFs set forth in Section V, A4, and must be alarmed in accordance with Section IV and be located in a building that has all of the following:

(1) Continuous personnel access control;

(2) A 24-hour guard force capable of responding to an alarm within five minutes; and

(3) A reserve guard force available to assist the responding guard in an emergency.

(c) SCIFs within fenced, guarded military compounds or equivalent may use specifications indicated in Section V, A2, and must be alarmed in accordance with Section IV and be located in a building that has all the requirements cited by paragraph B2(b) above.

3. Continuous Operations

(a) The SCIF must meet the construction specifications as identified in Section V, A2, and have an alert system as stated in Section IV if visual security of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

(b) An adequate security/guard force must be available to respond to the SCIF within five minutes in an emergency.

(c) SCI should be stored in lockable containers. If the configuration of the material precludes this, then there must be an adequate, tested plan to protect, evacuate, or destroy the material in event of emergency or natural disaster.

4. Secure Working Areas

(a) The SCIF must meet the specifications as set forth in Section V, A2.

(b) The SCIF must be alarmed in accordance with Section IV.

C. SCI FACILITIES LOCATED IN THE UNITED STATES ABOVE OR COMPLETELY BELOW GROUND LEVEL:

1. Closed Storage

(a) The SCIF must meet the specifications as specified in Section V, A2, or meet open storage requirements.

(b) The SCIF must be alarmed in accordance with Section IV.

(c) SCI must be stored in GSA-approved security containers.

2. Open Storage

Open storage of SCI shall be avoided. When open storage is necessary, the SCIF must meet either:

(a) The construction specifications for vaults set forth in Section V, A1, and must be alarmed in accordance with Section IV; or

(b) The construction specifications for SCIFs as set forth in Section V, A2, and must be alarmed in accordance with Section IV and be located in a building that has all of the following:

(1) Continuous personnel access control;

(2) A 24-hour guard force capable of responding to an alarm within five minutes;

(3) A reserve guard force available to assist the responding guard in an emergency.

3. Continuous Operation

(a) The SCIF must meet the construction specifications as identified in Section V, A2, and have an alert system as stated in Section IV if visual security of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

(b) An adequate security force must be available to respond to the SCIF within five minutes in an emergency.

(c) SCI should be stored in lockable containers. If the configuration of the material precludes this, then there must be an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster.

4. Secure Working Areas

(a) The SCIF must meet the specifications as specified in Section V, A2.

(b) The SCIF must be alarmed in accordance with Section IV.

D. SCI FACILITIES LOCATED OUTSIDE THE UNITED STATES:

The criteria for SCIFs outside the U.S. are the same as those for SCIFs within the U.S. except as follows:

1. Closed Storage

(a) The SCIF must meet the construction specifications for SCIFs as set forth in Section V, A3. No waiver shall be granted for this construction requirement. SCIFs within fenced, guarded military compounds or equivalent of "friendly" host countries, having armed, immediate response forces may use specifications indicated in Section V, A4, with prior approval of the SOIC.

(b) All SCI controlled material shall be stored in GSA approved security containers having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.

(c) The SCIF must be alarmed in accordance with Section IV.

2. Open Storage

(a) No waiver shall be granted for the construction requirement (Section V, A1) of a vault approved for open storage.

(b) Open storage of SCI will be permitted only for material which is of a size or configuration that precludes its being stored in the largest GSA-approved security container available. All other SCI must be stored in a GSA-approved security container having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.

(c) The SCIF must be alarmed in accordance with Section IV.

3. Continuous Operations

(a) The SCIF must meet the construction specifications as indicated in Section V, A3, and have an alert system as stated in Section IV if visual security of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

(b) In an emergency, all SCI must be stored in GSA-approved security containers, or the SCIF must have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster.

(c) SCIFs located on controlled military reservations or equivalent of "friendly" host countries, having armed, immediate response forces, may use secure area construction specifications as listed in Section V, A2, with prior approval of the SOIC.

SECTION IV
SECURITY ALARM REQUIREMENTS

A. All SCIFs, except those having continuous operation, must be alarmed. Continuous operation SCIFs will have an alert system if visual security of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

B. SCIFs located within the United States may use commercial monitoring facilities for alarm systems if approved by the CSA. Response to an alarm should not exceed 10 minutes or, when commercial central station is used, the requirements of UL repeated Class A service. (This response statement does not apply to "open storage" or "continuous operations" requirements that specify five minutes or less.)

C. SCIFs located outside the United States must have alarm systems monitored by SCI cleared personnel or U.S. citizens.

D. Alarm installation and maintenance should be accomplished by U.S. citizens. Use of foreign nationals for this purpose must have prior CSA approval and all work must be done under close supervision of SCI cleared personnel or U.S. citizens.

E. In SCIFs where the alarm transmission signal leaves the facility and traverses an uncontrolled area, Class A line supervision will be used. Class A line supervision is a wire-transmitted, non-repeatable, or encrypted signal, meeting the requirements of federal standard 1027.

F. In SCIFs where the alarm transmission signal does not leave a controlled area containing the SCIF, Class A or Class B line supervision may be used. Class B line supervision is a repeatable or unencrypted signal, wire transmitted.

G. All SCIF alarm systems will include the following:

1. Alarm components, when not specified by CSA, shall be UL approved.

2. Areas of the SCIF between the floor and ceiling shall be protected by volumetric sensors.

3. If a SCIF has a false ceiling or floor which provides a means for surreptitious entry, then one of the below listed methods must be used to protect that area:

(a) A separate alarm zone in secure mode at all times covering the area between the false and true ceiling or false and true floor.

(b) Construction of a physical barrier equal to the SCIF wall construction as set forth in Section V.

4. Perimeter doors will be protected by balanced magnetic switches.

5. All windows will be protected by an alarm system, either independent or by the volumetric sensors in the room, as determined by the CSA.

6. Emergency exits and secondary doors shall be on a separate zone from the motion detecting and main entrance sensors within the same SCIF.

7. Every SCIF shall be on a separate system.

8. If a SCIF consists of more than six rooms, or more than 5,000 square feet, then it shall be protected by two or more alarm zones as determined by the CSA.

9. All alarm control units will be located within the SCIF.

10. All alarm sensors will be tested monthly, i.e., door opened and volumetric sensors walk-tested. Test procedures will be prepared and recorded by the SCIF security officer or as directed by the CSA.

11. All components shall be installed in a manner to prevent access or removal from a location external to the protected zone.

12. All alarm systems shall be capable of operating from commercial AC power. In the event of commercial power failure, provisions will be made for automatic switch over to emergency power, and back to commercial power without causing an alarm. A signal will be presented to the monitor location indicating when the system has lost all power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. Emergency power must be capable of operating the system for a minimum of eight hours.

13. Volumetric sensors employed in the alarm system must be placed so that the most likely paths of an intruder are detected.

14. All sensors and control units will be equipped with tamper detection.

H. Details concerning classes of electronic line supervision, equipment type, specific component application and response/service requirements will be addressed in the technical annex attached or furnished by the CSA.

I. Alert System--An Alert System shall consist of balanced magnetic switches or other appropriate sensors on all entrances and passages or other areas where undetected entry could occur. These sensors shall be connected to a signaling device through a closed loop to a latching relay. Neither the signaling device relay nor the wire connecting the switches shall leave the SCIF.

SECTION V
CONSTRUCTION

A. SPECIFICATIONS:

1. Vault Construction Criteria:

(a) Reinforced Concrete Construction:

Walls, floor, and ceiling shall be a minimum thickness of eight inches of reinforced concrete. The concrete mixture shall have a comprehensive strength rating of at least 3,000 psi. Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8 inches in diameter, positioned centralized in the concrete pour and spaced horizontally and vertically six inches on center; rods will be tied or welded at the intersections. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

(b) Modular vaults meeting U/L standards may be used in lieu of 1.(a) above.

(c) Steel-lined Construction:

Where unique structural circumstances do not permit concrete construction of a vault, construction will be of steel alloy-type, such as U.S. Steel T-1, having characteristics of high yield and tensile strength. (If alloy-type steel is not available, normal structural steel may be used, but in a minimum thickness of 1/4 inch). The metal plates are to be continuously welded to

load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than six inches of reinforced concrete, then a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

(d) All vaults shall be equipped with a GSA approved Class 5 vault door. Normally, within the U.S. a vault shall have only one door which serves as both entrance and exit from the SCIF. If the "travel distance" from the most remote point in the SCIF to the door exceeds 50' a second door, equal to the original door, must be installed for life safety purposes. Travel distance shall be measured on the floor along the natural path of travel, starting one foot from the most remote point, curving around any corners or obstructions, and ending at the entrance doorway. When a SCIF has more than one door, only one should be used for normal business.

2. SCIF Construction Criteria:

Walls, floor, and ceiling to be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction must be done in a workmanlike manner, properly finished and/or painted. This facility is acceptable for the following:

(a) Inside the United States-Ground Level:

(1) Closed Storage, on a military installation or equivalent.

(2) Open Storage, on a military installation or equivalent, if facility is alarmed and located in a building that has continuous personnel access control, 24-hour guard force and reserve guard force.

(3) Continuous Operations

(4) Secure Working Area

(b) Inside the United States-Above or Below Ground Level:

(1) Closed Storage

(2) Open Storage, if facility is alarmed and located in a building that has continuous personnel access control, 24-hour guard force and reserve guard force.

(3) Continuous Operations

(4) Secure Working Area

(c) Outside the United States:

Continuous Operations, on a military reservation or equivalent, with prior approval of the SOIC.

3. SCIF Construction Criteria Which Requires:

Walls, ceilings, and floors shall be reinforced on the inside with steel plate not less than 1/8" thick. The plate at every vertical joint are to be affixed to vertical steel members of a thickness not less than that of the plate. The vertical plates shall be spot welded to the vertical members by applying a 1" long weld every 12"; meeting of the plates in the horizontal plane shall be continuously welded. Floor and ceiling reinforcements must be securely affixed to the walls with steel angles welded or bolted in place. Walls, ceiling and floors of reinforced concrete at least 4" thick or of solid masonry (stone or brick) at least 8" thick are adequate. Existing walls, ceilings, and floors of hollow masonry (blocks and tiles) or lesser materials not meeting this criteria must be reinforced with steel plating 1/8" thick. This facility is acceptable for the following overseas applications:

(a) Outside of the United States:

(1) Closed Storage

(2) Continuous Operations

(b) Inside the United States:

Not Applicable

4. SCIF Construction Criteria Which Requires:

Walls to be reinforced, slab to slab, with 9 gauge expanded metal. The expanded metal will be spot welded every 6" to metal supports of equal or greater thickness that have been solidly and permanently attached to the true floor and true ceiling. Floors and ceilings that are of masonry or metal construction require no special treatment. This facility is acceptable for the following applications:

(a) Inside the United States - Ground Level:

(1) Closed Storage

(2) Open Storage, if facility is alarmed and located in a building that has continuous personnel access control, 24-hour guard force and reserve guard force.

(b) Outside of the Unites States:

Closed Storage, on a military reservation or equivalent, with prior approval of the SOIC.

B. MINIMUMS:

The above provides minimum specifications. The use of materials having thickness or diameters larger than those specified is permissible. The terms "anchored to and/or imbedded into the floor and ceiling" may apply to the affixing of supporting members and reinforcing to the true slab or to the most solid surfaces; however, subfloors and false ceilings are not to be used for this purpose.

C. WINDOWS:

1. All windows which might reasonably afford visual surveillance of activity within, shall be made opaque or equipped with blinds, drapes or other coverings to preclude such visual surveillance.

2. Inside the United States:

Windows at ground level or readily accessible from the ground normally will be equipped with metal grills or bars. SCIFs located within fenced and guarded military compounds or equivalent may eliminate this requirement if the windows are made non-openable by either permanently sealing them or equipping them on the inside with deadbolt locking mechanisms. For SCIFs having open storage and/or located in a high crime or risk area, or in one that is subject to civil disorders, metal grills or bars will be used. Windows above ground level and not accessible need only be lockable from the inside with deadbolt lock mechanisms. In open storage conditions at ground level, consideration should be given to sealing the windows by filling with brick/mortar or affixing lockable steel shutters to the windows.

3. Outside of the United States:

All windows will be protected against forced entry with steel bars, except when located within fenced and guarded military compounds or equivalent where the CSA may waive this requirement.

D. MINIMUM SPECIFICATION FOR ENTRANCE, EXIT, AND ACCESS DOORS:

1. All doors must be plumbed in their frames and the frame firmly affixed to the surrounding wall.

2. All SCIF entrance doors must be equipped with a door closer, Group I combination lock, and an access control device. Doors with hinges exposed must be modified with non-removable pins or by installation of "dog bolts" or security studs. (NOTE: The specification does not apply to the GSA-approved Class 5 and 6 vault doors. These doors are secure as designated, must be used as specified in this document, and are not suitable for the installation of door closers, access control devices or panic hardware.)

3. SCIF exit doors, when required, must be the same, or equal to the entrance door. The door will be secured with "deadbolt" panic hardware on the inside and have no exterior hardware. Where life-safety codes permit, a sliding "deadbolt" should be installed, in addition to the panic hardware, and secured when the SCIF is unoccupied.

4. For entrance and exit doors, when life-safety codes dictate that panic hardware must exist on this door and the normally accepted extension #50 escape device is disallowed, an additional like door with out frontal hardware will be installed to facilitate the use of panic hardware.

5. Details of specific manufacturers and models of approved combination locks, access control devices and other related hardware is covered by technical annex furnished by CSA.

6. SCIFs Inside the United States may be equipped with either a Class 5 or 6 vault door; a metal-clad fire door, minimum of 16-gauge metal; a solid core wood door, minimum of 1 3/4 inch; or flat-sill fire door with built-in boltwork.

7. SCIFs Outside the United States must be equipped with a GSA-approved Class 5 or 6 vault door, or a locally fabricated door and frame equal to the steel reinforcement required in Section V, A3 or A4, depending on SCIF NOTE: Specifications for locally fabricated doors is covered by the technical annex furnished by CSA.

E. PHYSICAL PROTECTION OF VENTS AND DUCTS:

1. All vents, ducts, and similar openings in excess of 90 square inches that enter or pass through a SCIF must be blocked with either bars, grills, or commercial metal duct sound baffles that meet one of the sound attenuation classes. If bars are used, they must be 1/2 inch diameter steel welded vertically and horizontally 6 inches on center; if grills are used, they must be of 9-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms must be metal, permanently installed and no farther apart than 6 inches in one dimension.

2. All vents and ducts must have a non-conductive section (a piece of dissimilar material unable to carry electric current) installed at the perimeter of the SCIF. An access port to allow inspection of the protection in the vent or duct must be installed inside the secure perimeter of the SCIF. The access port itself must be able to be secured by padlock or other approved device.

3. SCIFs Located Inside the United States:

An alarm may be installed in lieu of bars or grills, depending on requirements of the CSA. Sound Baffles may also be required by the CSA.

4. SCIFs Located Outside of the United States:

Bars of 1/2 inch diameter steel, welded vertically and horizontally, 6 inch on center, must be used in addition to other requirements of the CSA.

SECTION VI
TEMPORARY SECURE WORKING AREA (TSWA)

During the entire period the TSWA is in use, the entrance will be controlled, and access limited to persons having the clearance for which the area has been approved. Approval for using such areas must be obtained from the SOIC of the next higher level within appropriate SCI channels, setting forth room number(s), building, location, purpose, specific security measures employed during usage as well as during other periods. TSWA's should be covered by an alarm system, where possible. These areas will not be used for periods exceeding an average total of 40 hours per month. No special construction is required other than to meet sound attenuation requirements. If such a facility must also be used for the discussion of SCI, a TSCM survey shall be conducted periodically on a random basis during the operation of the temporary facility.

SECTION VII
TELEPHONE SECURITY

Specific detailed instructions explaining the security measures that are mandatory for SCIFs, and the options available for implementing them, are provided in the "TELEPHONE SECURITY" technical annex to this directive.

The on-hook telephone audio security requirements for SCIFs are based on applications of technical standards developed and published by the Telephone Security Group (TSG). As the successor to the Telephone Security Panel (TSP), TSG is the primary technical and policy resource in the US Intelligence Community for all aspects of the Technical Surveillance Countermeasures (TSCM) program which involve telephones and/or telephone systems.

New TSG technical standards are developed, and existing ones are updated, to extend the benefits obtained from ongoing studies and research programs. It is essential that all utilizations of this section employ only the latest issues of applicable TSG standards. Only facilities which conform to the standards current at the time of installation will qualify for accreditation and grandfathering. When using the TELEPHONE SECURITY annex, inquiry should be made to assure that the latest versions of the TSG standards are available and to determine if there are any additional ones, not listed in the annex, which might be used to advantage. Questions relating to the TSG standards may be directed to the inquiring agency's TSG representative.